"Your logo here"

[Insert Cover Picture]

Interfaith Community Tabletop Exercise

Situation Manual

[Insert Date]

[Insert Caveat]

This Situation Manual (SitMan) provides exercise participants with all the necessary tools for their roles in the exercise. Some exercise material is

Photo Courtesy of [insert source]

intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

This page is intentionally left blank.

Exercise Agenda

Start Time	End Time	Activity
8:00 a.m.	8:15 a.m.	Welcome and Introductions
8:15 a.m.	9:15 a.m.	Module One: Pre-Incident Information Sharing
9:15 a.m.	9:30 a.m.	Break
9:30 a.m.	10:30 a.m.	Module Two: Incident
10:30 a.m.	10:45 a.m.	Break
10:45 a.m.	11:45 a.m.	Module Three: Recovery
11:45 a.m.	12:30 p.m.	Hot Wash / Closing Remarks

**All times are approximate*

This page is intentionally left blank.

EXERCISE OVERVIEW

Exercise Name	Interfaith Community Tabletop Exercise (TTX)
Exercise Dates	[Indicate the start and end dates of the exercise]
Scope	This exercise is a TTX planned for [insert exercise duration] and will focus on [insert scope]. This exercise was developed using materials created by the Cybersecurity and Infrastructure Security Agency (CISA) for a CISA Tabletop Exercise Package (CTEP).
Mission Area(s)	Prevention, Protection, Mitigation, Response, and Recovery [Select appropriate Mission Areas]
Capabilities	• Cybersecurity • Economic Recovery • Health and Social Services • Intelligence and Information Sharing • On-Scene Security, Protection, and Law Enforcement • Operational Communications • Operational Coordination • Planning • Public Health, Healthcare, and Emergency Medical Services (EMS) • Public Information and Warning • Situational Assessment • [Insert additional capabilities as necessary]
Objectives	1. Examine threat and incident information sharing, notification, and communication procedures between public and private sector partners, with a focus on intelligence community partners and faith-based organizations (FBO)s. 2. Examine private sector policies and procedures in response to a cyber-based attack. 3. Examine public and private organization response procedures, interaction, and public relations collaboration during an active threat at an FBO. 4. Discuss recovery and continuity plans and procedures

	following a complex coordinated attack. [Insert additional exercise objectives as necessary.]
Threat or Hazard	Phishing Attack, Vehicle Ramming, Active Shooter, and potential Improvised Explosive Device (IED)
Scenario	An interactive, discussion-based exercise focused on a vehicle ramming and active shooter. The scenario consists of three modules: Pre-Incident Information Sharing, Incident Response, and Recovery.
Sponsor	[Insert the name of the sponsor organization as well as any grant programs being used, if applicable]
Participating Organizations	[Please see Appendix B.]
Point of Contact (POC)	[Insert the name, title, agency, address, phone number, and email address of the primary exercise POC (e.g., exercise director or exercise sponsor).]

General Information

Exercise Objectives and Capabilities

The exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to capabilities, which are the means to accomplish a mission, function, or objective based on the performance of related tasks, under specified conditions, to target levels of performance. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team (EPT).

Exercise Objectives	Capability
Examine threat and incident information sharing, notification, and communication procedures between public and private sector partners, with a focus on intelligence community partners and FBOs.	✓ Intelligence and Information Sharing ✓ Operational Communications ✓ Planning
Examine private sector policies and procedures in response to a cyber-based attack.	✓ Cybersecurity
Examine public and private organization response procedures, interaction, and public relations collaboration during an active threat at an FBO.	✓ On-Scene Security, Protection, and Law Enforcement ✓ Operational Coordination ✓ Operational Communications ✓ Planning ✓ Public Health, Healthcare, and EMS ✓ Public Information and Warning
Discuss recovery and continuity plans and procedures following a complex coordinated attack.	✓ Economic Recovery ✓ Health and Social Services ✓ Public Information and Warning
[Insert objective]	✓ [Insert capability aligned to each objective]

Table 1. Exercise Objectives and Associated Capabilities

Video Use Guidelines

This SitMan includes optional videos embedded throughout the scenario for use in the exercise to accompany the narrative. Videos can be used to engage stakeholders during a tabletop exercise by simulating news coverage of incidents. Use of the video links is recommended and coinciding transcripts are included in **Appendix A,** but the scenarios are written in narrative format for use if the exercise does not allow for video use.

Videos are embedded using hyperlinks which will route the user directly to the corresponding YouTube video. For best results, the EPT should prepare reliable internet access with unrestricted access to YouTube.com, a way to share the videos with exercise participants, audio output equipment, and consider the following list of best practices:

- Familiarize the facilitator with video functionality to ensure smooth transitions during exercise conduct or designate an EPT member to run the slides.
- Open all videos in advance of the exercise to mitigate any technical issues that may arise from opening the videos on the spot.
- Ensure all participants have a copy of the SitMan for use in the event of technical difficulties.
- Determine whether to allow participants to review videos prior to exercise conduct.

Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

- **Players** are personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
- **Observers** do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
- **The Facilitator** provides situation updates and moderates discussions. They also provide additional information or resolve questions as required. Key EPT members also may assist with facilitation as subject matter experts (SMEs) during the exercise.

- **Moderators** are responsible for admitting and signing in all participants to the virtual exercise, monitoring the chat area for questions and / or issues, and controlling participant audio.
- **Evaluators** are assigned to observe and document the discussion during the exercise, participate in data analysis, and assist with drafting the After-Action Report (AAR).

Exercise Structure

This exercise will be a discussion-based, facilitated exercise. Players will participate in the following three modules:

- Module One: Pre-Incident Information Sharing
- Module Two: Incident
- Module Three: Recovery

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in discussions of appropriate [insert mission area] issues.

Exercise Guidelines

- This exercise will be held in an open, no-fault environment wherein capabilities, plans, systems, and processes will be evaluated. Varying viewpoints, even disagreements, are expected.
- Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
- Decisions are not precedent setting and may not reflect your jurisdiction's / organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
- Issue identification is not as valuable as suggestions and recommended actions that could improve [insert mission area] efforts. Problem-solving efforts should be the focus.
- The assumption is that the exercise scenario is plausible, and events occur as they are presented. All players will receive information at the same time.

Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned core capabilities. Players will be asked to complete a participant feedback

form. These documents, coupled with facilitator observations and evaluator notes, will be used to evaluate the exercise and then compiled into the AAR / Improvement Plan (IP).

This page is intentionally left blank.

MODULE ONE: PRE-INCIDENT INFORMATION SHARING

Scenario

[Insert Location]

[Insert Month, Day, Year]: [Insert Time]

Based on an increased amount of online chatter from the domestic extremist group, Universal Adversary (UA), calling for attacks on large public gatherings across the Unites States, the Secretary of Homeland Security, in coordination with other federal entities, issues an "Elevated" Threat Alert through the National Terrorism Advisory System (NTAS), warning of a credible domestic terrorist threat in states in identified areas. There is no information available at this time that would warrant the release of an "Imminent" Threat.

The alert states the threat is from an extremist group in the United States that focuses on mass gatherings, particularly at places of worship and interfaith gatherings. The alert is to remain in place until further notice.

Discussion Questions

1. How would your organization receive intelligence and protective measures information?
    a. What organization would you communicate with (e.g., local law enforcement agencies, Federal Bureau of Investigation [FBI], etc.)?
    b. Does your organization maintain a relationship with your Department of Homeland Security (DHS) Protective Security Advisor (PSA)? If so, do you have a rapid means of contacting them?
    c. Does your organization use the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) portal?
    d. How does your organization triage the information you receive (e.g., formal reporting, rumors, social media) for further dissemination within your organization and to your staff and congregants?
        i. Given current information sharing procedures, what types of official information are the most useful (e.g., immediate information versus analyzed information) to your organization?

ii. Does your organization perform independent analysis on information provided? If so, describe the process.

2. What information sharing and dissemination processes does your organization currently have to alert your staff and your congregants to an incident?
    a. What notification capabilities (e.g., alerts, emails, telecom, text messages, special tools) do you use to share information and communicate protective measures implementation?
    b. Are there technological barriers, legal considerations, or institutional sensitivities that might affect information sharing, such as religious customs that prohibit use of electronic communication during specific times?
        i. If so, how will threat-based alerts and notifications be distributed to community members who follow religious customs that prohibit the use of electronic communication during specific times?
3. If your organization receives information related to potential threats against your facilities and personnel, how would you communicate this information to the appropriate entities (e.g., local law enforcement agencies, FBI, your DHS PSA, etc.)?
4. If there is identified "suspicious behavior" observed at one of your organization's locations, how does staff report this information to law enforcement officials and other members of your organization?
    a. How are suspicious behavior trends tracked across your faith on a national level?
    b. Is your organization aware of the "If You See Something, Say Something™" campaign or the National Suspicious Activity Reporting (SAR) Initiative?
5. In the event of evidence of a credible threat to the facilities or people of your faith, what protective security measures or recommendations, if any, will be employed at your organization?
    a. Does your organization review your emergency response plans (e.g., site security plans, emergency occupancy plans, emergency action plans, or other appropriate plans)?
    b. Do you coordinate protective measure implementation with any other organization within your faith?
    c. Do you coordinate protective measure implementation with government entities, such as law enforcement agencies and your DHS PSA?

d. Are you aware of the information bulletins and advisories DHS provides that recommend protective measures (e.g., a Joint Intelligence Bulletin [JIB])?

Module Two: Incident Response

Scenario

[Insert Location]

[Insert Month, Day, Year + 2 Weeks]: 6:00 a.m.

Local law enforcement identifies information posted online regarding your facility that could only have been obtained directly from your organization. Upon preliminary investigations, your staff identifies several email accounts that phishing attacks compromised.

[Insert Month, Day, Year + 2 Weeks]: 7:30 a.m.

While the extent of the data breach is not yet known, the current investigation has revealed that confidential personnel records were among the files accessible to the attackers. It has also been determined that over the last several months, there were a series of phishing attempts to gain access to your internal systems, including the personal emails of leadership, special events calendars, and congregation members' personally identifiable information (PII).

There have been at least two successful breaches, which extracted member contact information and the special events calendar. Some of your congregants report they've received suspicious e-mails and posts to their social media, and some members have raised concerns about some suspicious activities at their homes.

Click here for Video Supplement #1 [1] *or follow the transcription in Appendix A.*

Discussion Questions

1. How would this cybersecurity incident be handled? What notifications would be made?
2. From which sources does your organization receive cybersecurity threat intelligence? For example, information from CISA, FBI, open-source reporting, security service providers, or others?
    a. What cyber threat information is most useful?
    b. Is the information you receive timely and actionable?
    c. Who is responsible for collating information across your organization?

[1] Video supplement #1: https://www.youtube.com/watch?v=TZQXmcfJqIg&list=PL-BF3N9rHBLJHp2wln3O6l6egVofFeS-p&index=1

3. Does your organization provide basic cybersecurity and / or IT security awareness training to all users (including managers and senior executives)?
    a. How often is training provided?
    b. Does the training cover:
        i. Reviewing organizational acceptable use and IT policies?
        ii. Awareness of prominent cyber threats?
        iii. Password procedures?
        iv. Whom to contact and how to report suspicious activities?
    c. Is training required to obtain network access?
    d. What security-related training does your organization provide to, or contractually require of, IT personnel and vendors with access to your organization's information systems?
    e. How often do they receive that training?
4. How do employees report suspected phishing attempts?
    a. What actions does your department take when suspicious emails are reported?
    b. Are there formal policies or plans that would be followed?
    c. Does your organization conduct phishing self-assessments?
5. Has your organization conducted a cyber risk assessment to identify organization-specific threats and vulnerabilities?
    a. What are your most significant threats and vulnerabilities?
    b. What are your highest cybersecurity risks?
6. Does your IT department have a patch management plan? If so:
    a. Are risk assessments performed on all servers on the network?
    b. Do processes exist to proactively evaluate each server's criticality and applicability to software patches?
    c. Does this plan include a risk management strategy that addresses the following considerations?
        i. The risks of not patching reported vulnerabilities
        ii. Extended downtime
        iii. Impaired functionality
        iv. Data loss

Scenario Update

[Insert Location]

[Insert Month, Day, Year + 2 Weeks]: 6:00 p.m.

It is a sunny evening, and your organization is hosting an outdoor interfaith event, [insert event name], that is underway. Many members of your congregation are enjoying a relaxing evening with friends, family, and congregants from houses of worship in other areas. A few congregants report to event organizers that they have noticed a small unmanned aerial vehicle (UAV) hovering above the event space. No one can be seen in the area controlling the drone, and the drone flies off shortly after it is reported to event organizers.

[Insert Month, Day, Year + 2 Weeks]: 6:30 p.m.

Suddenly, a large truck accelerates and drives off the road near the gathering area and your building facility. It strikes numerous people before colliding into the entrance of the building. As uninjured people help those the truck struck, two individuals exit the vehicle with semi-automatic rifles and begin firing indiscriminately into the crowd as they make their way into your facility. Panicked attendees begin fleeing in every direction as numerous people lay scattered about, injured from both the vehicle ramming and subsequent gunfire.

Click here for Video Supplement #2 [2] *or follow the transcription in Appendix A.*

[Insert Month, Day, Year + 2 Weeks]: 7:00 p.m.

Responding police engage the shooters and quickly neutralize the assailants. They begin securing the scene when they discover two duffel bags in the rear of the vehicle. Initial reports estimate [insert number] people were injured or killed in the attacks. As news of the incident begins to break, people calling to ask about loved ones overwhelm the local 911 centers and your organization's phone lines.

Click here for Video Supplement #3 [3] *or follow the transcription in Appendix A.*

Discussion Questions

1. Do facility incident response plans (e.g., site security plans, emergency action plans, emergency response plans, or other appropriate plans) contain protocol for responding to an active shooter / vehicle ramming?

[2] Video supplement #2: https://www.youtube.com/watch?v=CrDi6m75q4M&list=PL-BF3N9rHBLJHp2wln3O6l6egVofFeS-p&index=2
[3] Video supplement #3: https://www.youtube.com/watch?v=gESe-h1FtB0&list=PL-BF3N9rHBLJHp2wln3O6l6egVofFeS-p&index=3

a. Is staff trained for this type of emergency incident?
    i. Is emergency contact information made available to the call desk?
    ii. Do procedures exist for sheltering-in-place versus evacuation?
b. Do you have notification systems to warn staff and congregants both on-site and off-site during such an incident?
c. Is there a way to account for staff (i.e., those who reported for work that day versus those on leave)?
d. What does the facility emergency coordinator need to consider (e.g., injuries, evacuation routes, hospitals)?
e. What procedures exist to manage the threat the UAV poses?
f. What other life safety issues should be considered?

2. Is there security on-site at your facility?
    a. How is security trained to respond to this type of incident? What are their roles and responsibilities?
    b. Do security personnel and first responders have interoperable radios / communication? Are there plans for agencies to communicate if they cannot communicate via radio?
3. Is security clearly identifiable upon law enforcement's arrival? Does your facility have physical security measures that may be relevant to this scenario?
    a. Is there any type of perimeter security (e.g., fences, doors, gates)?
    b. What types of vehicle control checkpoints are present (e.g., barriers, driveways, parking lots)?
    c. Does the public have access to the facility?
4. How is the emergency response coordinated?
    a. Are any of the facility's incident response plans provided to first responders prior to potential incidents?
        i. If not, how is key information communicated to them during the incident response?
    b. If there are locked doors or other physical barriers, how do emergency response personnel access the buildings?
        i. Upon arrival of law enforcement, is there a "go bag" available to them containing desired items such as a facility map / floor plans, access swipe cards, elevator keys, etc.?

ii. Is law enforcement familiar with your facility?

c. Are there any safety or religious concerns for first responders that need to be addressed (e.g., entering restricted, hazardous, or religiously sensitive areas)?

d. Have local first responders participated in exercises and / or training at your facility?

e. Do you know the specific local law enforcement policies and procedures regarding active shooter incidents for your area?

f. How is response coordinated, and who maintains decision-making authority if management is not available?

i. Does the security plan, or any other plan, capture the delegation of authority?

g. Is there a safe location identified for people who are evacuating the immediate area?

5. How are communications related to the emergency handled?

a. Who is in charge of ensuring that staff and congregants are informed of the status of events?

b. What are your organization's information sharing responsibilities during the response to the incident?

c. At what point do you begin sharing information with other members of your FBO?

d. How will your organization interact with media representatives and control media access to the facility?

e. Are there established procedures to manage the media when they arrive?

f. Should additional emergency announcements be made to the public?

6. How do state and local officials coordinate their response to an incident at the facility?

a. Do you have memorandums of understanding (MOU) or memorandums of agreement with any local, regional, or state response agencies?

b. What incident response plans do local, county, and state law enforcement agencies have for an active shooter / improvised explosive device (IED) situation? Who leads the response?

c. What would state and local officials need from your organization during an incident like the one detailed in this module?

7. Following the incident, what measures would local law enforcement take to protect your organization (e.g., outreach, increased vigilance, etc.)?
8. What assistance is available for staff and congregants following this event?
    a. How is information communicated during the days following the incident?
    b. Will counseling for members of your faith be available?
    c. Will there be any financial assistance or benefit programs for staff if the facility is shut down on a temporary basis?
    d. What is the procedure if injuries received on the job hospitalized a staff member?
9. Do the facility's incident response plans adequately address the emergency response and coordination activities described in the module? If not, what can be improved?

This page is intentionally left blank.

MODULE THREE: RECOVERY

Scenario

[Insert Location]

[Insert Month, Day, Year + 2 Weeks]: 8:00 p.m.

Law enforcement have secured the scene, and an investigation into the attack is underway. Bomb technicians have cleared the vehicle the assailants drove, and victims of the attack have been transported to local hospitals. Preliminary investigations have identified that the perpetrators may have had access to and used internal security footage from your facility, both during the incident and potentially beforehand, as reconnaissance. It is still unconfirmed whether this attack is related to the earlier data breach. However, law enforcement has stated that this is an isolated incident and that there is no further threat to your congregation.

Click here for Video Supplement #4 [4] *or follow the transcription in Appendix A.*

[Insert Month, Day, Year + 1 Day]: Following Morning, 8:00 a.m.

The investigations continue, and the local community, as well as the interfaith community nationwide, is still in shock that an incident like this could occur. Some members foster a sense of outrage. Social media is running rampant with rumors and misinformation regarding the attacks, including images and videos from eyewitnesses. Calls from individuals looking for information on their loved ones are still inundating your organization's phone lines and 911 call centers. Additionally, seeing as the data breach led to the loss of confidential information, members of your congregation are demanding answers regarding what steps are being taken to ensure their personal safety.

Click here for Video Supplement #5 [5] *or follow the transcription in Appendix A.*

Discussion Questions

1. Does your organization have a business continuity or continuity of operations plan?
    a. Does your continuity of operations plan include a crisis communications plan?

[4] Video supplement #4: https://www.youtube.com/watch?v=iGQrdSEVVlE&list=PL-BF3N9rHBLJHp2wln3O6l6egVofFeS-p&index=4
[5] Video supplement #5: https://www.youtube.com/watch?v=M0cE_tCgvlQ&list=PL-BF3N9rHBLJHp2wln3O6l6egVofFeS-p&index=5

2. How and what type of messaging will be sent to congregants and the surrounding community?
    a. What training do employees receive regarding media relations and the release of sensitive information?
3. What are the priorities at your facility or organization post-incident?
    a. Do your plans, policies, or procedures specify these priorities?
    b. How are these priorities communicated internally?
    c. Are priorities coordinated with county emergency management?
    d. Are priorities coordinated with state or federal agencies?
    e. What coordination with national or international faith leaders will take place?
4. What mental health services are available for congregants, employees, and responders?
    a. What standard operating procedures (SOPs) are in place for assisting visitors that the incident impacted?
    b. How would available services be communicated?
5. Are there plans to handle donations management after the incident? Who is responsible for this task?
6. Are there plans to handle memorials after the incident? Who is responsible for this task?
7. What local, state, or federal resources are available to assist in recovery or business continuity efforts?
    a. Does your facility have MOUs with local response agencies or other FBOs?
8. How is information communicated with personnel and families during the days following the incident?
9. What information are you communicating with the public?
    a. Who in your organization is responsible for making this communication?
    b. How is your facility adapting messaging to ensure congregants and their families still feel safe?
        i. Do your plans, policies, and procedures outline this?
10. Do recovery procedures affect nearby FBOs in any way?
11. Is social media being monitored to maintain awareness of information spreading that may not be accurate?
    a. Who is responsible for this?

b. What procedures exist to counter false information?

12. What is the plan to handle the significant media attention from national and international outlets?

13. At what point would you consider your organization back to steady-state operations?

14. What actions would be taken to address security concerns at other FBOs following the incident?

APPENDIX A: SUPPLEMENTAL VIDEO TRANSCRIPTS

Video Supplement #1: 7:30 a.m. – News Update

Click here for Video Supplement #1 [6] *or follow the transcription below.*

News Anchor: Welcome to Action News. I'm Megan Lee. This morning we are reporting on what appears to be a large, sophisticated phishing attack directed against interfaith communities. Details remain sketchy as investigators are trying to determine the full extent of the breach.

What we can report is that phishing emails were sent over the last several months to many members of the interfaith-based leaders, with at least two successful breaches providing an unknown level of access to internal networks, extracting contact information and vital records on members from the interfaith-based communities. The purpose and motives are unknown, but what officials are saying is that it was deliberate and targeted, which raises concerns for security issues and law enforcement.

We have our reporter, Andreas Smith, at the organization with their comment from their spokesperson. Andreas?

News Correspondent, Andreas Smith: Thanks, and as you reported earlier, there was a computer systems breach at the interfaith organization. I'm here with an organization spokesperson. Can you tell me about the breach?

Interfaith Spokesperson: We can confirm that our community has experienced a series of phishing attempts to gain access to our data system, the personal emails of leadership, the calendar of special events, and congregation members' information.

At the present time, there have been at least two successful breaches, extracting members' contact information and our special events calendar. Our organization is working with authorities investigating this breach and has reached out to all of our members, partnerships, and as well as our stakeholders. We've asked everyone to be vigilant in following strict security measures.

We also have additional concerns that some of our members are reporting having received suspicious emails and posts to their social media accounts, and some members have raised concerns about some suspicious activities at their home addresses. Our organization, along with our partners, are working closely with law enforcement, as well as the FBI, to ensure the safety of our members and to help apprehend those responsible.

[6] Video supplement #1: https://www.youtube.com/watch?v=TZQXmcfJqIg&list=PL-BF3N9rHBLJHp2wln3O6l6egVofFeS-p&index=1

News Correspondent, Andreas Smith: Thank you for your time. Back to you in the studio.

Video Supplement #2: 6:30 p.m. – Breaking News

Click here for Video Supplement #2 [7] *or follow the transcription below.*

News Anchor: Breaking news just coming in. Action News has learned of an attack at a community center where an interfaith event is being held. Hi, I'm Megan Lee.

[7] Vidoe https://www.youtube.com/watch?v=CrDi6m75q4M&list=PL-BF3N9rHBLJHp2wln3O6l6egVofFeS-p&index=2

At this hour, police are on the scene of a deadly shooting at the community center. According to police officials, at approximately 6:15 p.m. this evening, a large vehicle deliberately sped into a crowd of men, women, and children participating in an outdoor celebration at the community center. Two gunmen then exited the vehicle with semi-automatic rifles and began shooting into the crowd, resulting in numerous injuries and possible fatalities.

This incident comes just days after a computer system network breach was reported by the organization hosting the interfaith event. As reported earlier this week, the organization reported at least two network system breaches compromising numerous records. Forensic computer investigators have begun working with the organization to investigate the targeted information to include membership contacts, special event calendars, and confidential organization information. At this time, we can only speculate that the breach and the shooting are related.

According to eyewitness accounts, at approximately 6:00 p.m. this evening, patrons of the interfaith community observed a drone flying in close proximity to the outdoor celebration. At about 6:15 p.m., a large panel truck left the road in front of the community center and accelerated into the crowd. The vehicle then proceeded to ram the front entrance, coming to a stop at the main entrance of the facility. Eyewitness accounts identified two masked individuals exiting their vehicle with semi-automatic weapons, randomly shooting attendees. Reports coming in are stating that there have been several casualties.

Stay tuned to Action News for the latest on the vehicle ramming and shooting at the interfaith event held at the community center.

Video Supplement #3: 7:00 p.m. – News Update

Click here for Video Supplement #3 [8] *or follow the transcription below.*

News Anchor: Thank you for staying with us for this breaking news. I'm Megan Lee. For those of you just joining us, there has been an attack at the community center where an interfaith event was being held.

It has been reported that two assailants carried out a violent attack at the community center. Local law enforcement and emergency responders have the scene blocked off from reporters and bystanders so they can continue to investigate the scene. Let's go to our field reporter, Andreas Smith, with the latest. Andreas?

[8] Video supplement #3: https://www.youtube.com/watch?v=gESe-h1FtB0&list=PL-BF3N9rHBLJHp2wln3O6l6egVofFeS-p&index=3

News Correspondent, Andreas Smith: We apologize if we are repeating any information but here is what we can report.

At approximately 6 p.m., a number of attendees at the community center interfaith celebration noticed a drone flying very close to the scene of the event. Shortly after, a large truck was seen exiting the road in front of the community center, striking people in its way, as it collided with the front entrance of the community center. Once the truck came to a stop, two masked shooters exited the vehicle with semi-automatic weapons, shooting patrons inside the community center as well as on the event grounds. We've heard that law enforcement exchanged gunfire with the suspected shooters, but we do not have any additional information at this time. We also don't know if there are additional suspects at large.

A few minutes ago, the bomb squad arrived on the scene. It's difficult to see from this angle, but bomb squad technicians are securing what appears to be two large duffel bags in the open back of the shooters' truck. We do not have much information on this; however, I can tell you that the police have their canine dogs going through the front and back of the truck.

While the truck continues to be searched, emergency responders continue to arrive at the scene, transporting the injured. Though we can't confirm it at this time, we suspect a high number of casualties and most likely some fatalities. We will stand by for the next update. Back to you.

News Anchor: Thank you, Andreas, for that report. Stay tuned to Action News for our continued coverage. I'm Megan Lee.

Video Supplement #4: 8:00 p.m. – News Update

Click here for Video Supplement #4 [9] *or follow the transcription below.*

News Anchor: We are minutes away from our next briefing on the vehicle ramming and shooting event at the community center. A police department spokesperson is about to give an address.

Police Department Spokesperson: As I am certain most of you are aware, at approximately 6:15 p.m. this evening, two assailants carried out a violent attack at the community center. Our initial investigation shows that two assailants, operating a large truck, purposely drove into a crowd with the intent on injuring as many people as possible, before ramming the truck into the front entrance of the center. We can confirm that two unidentified individuals exited the vehicle with semi-automatic weapons, opening fire on community center attendees internal and external to the building.

According to investigators, it appears as though the perpetrators may have had access and utilized internal security footage of the facility, both during

[9] Video supplement #4: https://www.youtube.com/watch?v=iGQrdSEVVlE&list=PL-BF3N9rHBLJHp2wln3O6l6egVofFeS-p&index=4

the attack and potentially beforehand, as reconnaissance. We cannot confirm at this time if there is a relationship to this attack and the data breach reported earlier. However, an initial search of the truck found printed photos and streaming feeds from inside the facility.

Local law enforcement was very quick to the scene, engaging with the shooters within five minutes. Both shooters have been neutralized by law enforcement. Local law enforcement forensic teams have joined forces with state and federal forensic and cyber agencies to determine if the phishing and computer system breach to the organization are related to the incident at the community center.

At this time, we do not expect any additional suspects in this horrible incident, however, we will continue our investigation with local, state, and federal resources. The injured have been transported to numerous area hospitals and medical centers throughout the city. A joint investigation with local, state, and federal law enforcement officials has been coordinated, as this attack is being reviewed as a probable hate crime. We will continue to investigate this incident and provide an update as more information becomes available. At this time, I cannot accept any questions. Thank you.

News Anchor: Just to recap, at approximately 6:15 p.m., two assailants carried out a complex violent attack at our local community center. Reports have identified two assailants, operating a large truck, leaving the street at high speeds, striking numerous people, before ramming into the facility during the interfaith event. Two assailants then exited the vehicle with semi-automatic weapons, shooting celebration attendees.

What makes this incident even more disturbing is that there may have been a connection to this event and the data breach that occurred earlier as potential surveillance, picking the right time to attack. Stay tuned for more as we continue to follow this horrible event. For Action News, I'm Megan Lee.

Video Supplement #5: 8:00 a.m. – News Update

Click here for Video Supplement #5 [10] *or follow the transcription below.*

News Anchor: You are watching Action News. I'm Megan Lee.

According to law enforcement officials, investigations continue. The attack fostered a sense of outrage within the interfaith community all over the nation as many of the families are still waiting to hear from loved ones who are missing. Social media has already been flooded with images and live-

[10] Video supplement #5: https://www.youtube.com/watch?v=M0cE_tCgvlQ&list=PL-BF3N9rHBLJHp2wln3O6l6egVofFeS-p&index=5

streaming videos from eyewitnesses as well as pleas for information regarding affected family members or loved ones.

APPENDIX B: EXERCISE PARTICIPANTS

Participating Private Sector Organizations
[Insert private sector participants]

Participating Local Organizations
[Insert local participants]

Participating State Organizations
[Insert state participants]

Participating Federal Organizations
[Insert federal participants]

Other Participating Organizations
[Insert other participants]

Other Participating Organizations

This page is intentionally left blank.

APPENDIX C: RELEVANT PLANS

[Insert excerpts from relevant plans, policies, or procedures to be tested during the exercise.]

This page is intentionally left blank.

APPENDIX D: ACRONYMS

Acronym	Term
AAR	After-Action Report
CISA	Cybersecurity and Infrastructure Security Agency
CTEP	CISA Tabletop Exercise Package
DHS	Department of Homeland Security
EMS	Emergency Medical Services
EPT	Exercise Planning Team
FBI	Federal Bureau of Investigation
FBO	Faith-Based Organization
HSIN-CI	Homeland Security Information Network – Critical Infrastructure
IED	Improvised Explosive Device
IP	Improvement Plan
JIB	Joint Intelligence Bulletin
MOU	Memorandum of Understanding
NTAS	National Terrorism Advisory System
PII	Personally Identifiable Information
POC	Point of Contact
PSA	Protective Security Advisor
SAR	Suspicious Activity Report
SitMan	Situation Manual
SME	Subject Matter Expert
SOP	Standard Operating Procedures
TTX	Tabletop Exercise
UA	Universal Adversary
UAV	Unmanned Aerial Vehicle

"Insert your logo here"